REMARKS

In response to the Official Action Advisory Action dated 1/22/2008 and dated 10/1/2007, applicant's counsel called the Examiner on 1/29/08 to discuss a typographical in Applicant's prior Remarks section submitted in the Amendment of 1/2/2008. Specifically, the reference on page 13 of Applicant's Remarks in the Amendment of 1/2/2008 inadvertently references **"[a first SSL connection]"** twice in the same paragraph, yet Applicants describe in the Amendment to the Specification and argue the referenced subject matter as first and second connections in remainder of the remarks.

This inconsistency was discussed with Examiner Williams. Accordingly, the cited paragraph should be presented for argument in the record as follows:

At page 6, lines 2-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification, the following is stated:

> The present invention is generally depicted in FIGS. 2A and 2B and is directed to a system and method for increasing data access in a secure socket layer network environment and is generally designated by the number 100. The system 100 includes a *web server computer 102* which has an operating system/software, server software, memory and linking devices as is known in the art. Further, the *computer 102 has SSL protocol server software operably disposed thereon for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key.*
>
> A *client computer 104* includes an operating system/software, web browser software having SSL protocol client software operably disposed *thereon for enabling a SSL connection*, memory and linking devices as is known in the art and is communicatively linked to the web server computer 102. SSL acceleration client (SSLAC) software is operably disposed on the client computer 104 for monitoring when the web browser requests a SSL connection with the web server 102.
>
> *SSL acceleration server (SSLAS) software is operably disposed on the web server computer 104 for receiving a request for a SSL connection through SSL acceleration client software.* The SSL acceleration server software is operably associated with the SSL protocol server software to obtain one either a copy or an equal credential of the CA

certificate (i.e., a pseudo CA certificate) and private key.

The operation of the invention can be understood from steps shown in FIGS. 2A and 2B. *SSL acceleration client software intercepts 200 new SSL request for a SSL secure connection from the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection.* The SSLAS then determines 204 which CA certificate is operably associated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. *At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection.* **[i.e., a first SSL connection]** *The SSLAC software sends 208 the copy of the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 102). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a "handshake" is completed and secure communications between the client computer's web browser and SSLAS software e* **[i.e., a second SSL connection]** *and by using the secret key, data can be accelerated between the client computer 104 and the web server computer 102 employing acceleration software, such as compression software of the SSL acceleration client/server software.*

Because the SSL connection is terminated by SSLAC, *SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream.* This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.

The specification clearly discloses a client computer, web server, first and second SSL connections wherein the second permits optimization techniques to be applied on the data transmitted through the second SSL connection. Accordingly, withdrawal of the rejection to the specification and drawings is kindly requested.

In view of this clarification, the prior above-identified amendment is submitted to be proper and does not raise a new matter issue. Rather, the Amendment is submitted to place the

application and claims in better condition for allowance. Entry of the prior amendment is kindly requested and review and reconsideration are requested in view of the above remarks.

Finally, the Advisory Action appears to maintain a position that since the prior art teaches multiple connections, this renders obvious the instant invention.

Applicants kindly traverse. In the cases disclosed by the prior art, each paradigm fails to show multiple SSL connections between the same client and server. Rather, there is simply shown the inclusion of the means to create a single secure connection between the client/relay and relay/server.

It is clear that Aziz only discloses making a single connection between each client and a relay and a relay and a server. Moreover, Aziz states that the connection can be a cleartext HTTP connection. This can be a problem and create a security issue because Basic credentials are Base64-encoded. If Basic credentials are sent over an HTTP connection, they may be read as clear text and decoded.

There is no disclosure, suggestion or teaching in Aziz as to the need or means how to make multiple SSL connections with the same client and same server. This is only taught by the present invention.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [paragraph 0015]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL

connection between the client and server as opposed to the instant invention which provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections through whereby data can pass in a compressed form, for example, in the second established connection. Gast teaches away from the instant invention.

Likewise as stated above, Aziz attempts leads toward offloading the SSL connection by using a cleartext HTTP connection, i.e., Aziz states "reducing the server workload even more compared to using previously negotiated SSL sessions". Combining the references in no way would result in the present invention and in fairly interpreting the teachings of each and combining such teachings a reasonable combination at best would be the combination of offloading encryption processing further with the aid of relays. This does not render the instant invention. Withdrawal of the rejection of claims under 35 U.S.C. 103 over Aziz in view of Gast is respectfully requested.

Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. Like Aziz, there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The present invention calls for a system

for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second SSL connection. A method employing these elements is also provided.

The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created. Freed et al., like Aziz, introduces a third element in the chain of connection and another potential break point for communication.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (or Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

It is respectfully submitted that the instant claimed invention is not taught, disclosed or suggested by Aziz, Gast or Freed et al. taken alone or together. The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of claims 1-19 is respectfully requested.

Therefore, allowance of claims 1-19 is requested at as early a date as possible. This is intended to be complete response to the Advisory Action of 1/22/2008 in furtherance of the Official Action dated 10/1/2007 which fell due on a holiday. It is not believed that any extension of time is due as the prior Amendment is deemed to have been proper, but to the extent that one is required, please charge account 500353 for the one month extension.

Respectfully submitted,

/R. William Graham/

R. William Graham, 33,891

Certificate of Transmission

I hereby certify that this correspondence is being electronically filed with the PTO for group 2137on the date shown below.

/R. William Graham/

Date. Tuesday, January 29, 2008 R. William Graham, 33,891